HSGW Configuration

This chapter provides configuration information for the HRPD Serving Gateway (HSGW).

Important Information about all commands in this chapter can be found in the *Command Line Interface Reference*.

Because each wireless network is unique, the system is designed with a variety of parameters allowing it to perform in various wireless network environments. In this chapter, only the minimum set of parameters are provided to make the system operational. Optional configuration commands specific to the HSGW product are located in the *Command Line Interface Reference*.

The following information is provided in this chapter:

Configuring the System to Perform as a Standalone HSGW

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an HSGW in a test environment. For a more robust configuration example, refer to the Sample Configuration Files appendix. Information provided in this section includes the following:

Information Required

The following sections describe the minimum amount of information required to configure and make the HSGW operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the HSGW in the network. Information on these parameters can be found in the appropriate sections of the *Command Line Interface Reference*.

Required Local Context Configuration Information

The following table lists the information that is required to configure the local context on an HSGW.

Required Information	Description
Management Interface Configuration	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface.Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17.A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Security administrator name	The name or names of the security administrator with full rights to the system.
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access that will be used to access the system such as telnetd, sshd, and/or ftpd.

Required HSGW Context Configuration Information

The following table lists the information that is required to configure the HSGW context on an HSGW.

Required Information	Description
HSGW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the HSGW context is recognized by the system.
Diameter authentication dictionary	The name of the Diameter dictionary used for authentication.
Diameter endpoint name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Diameter endpoint is recognized by the system.The Diameter endpoint name identifies the configuration used to communicate with the 3GPP AAA server in the AAA context.

Required Information	Description
Accounting policy name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the accounting policy is recognized by the system. The accounting policy is used to set parameters for the Rf (off-line charging) interface.
A10/A11 Interface Configuration (To/from eAN/ePCF)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system.Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface.Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17.A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
HSGW Service Configuration	
HSGW service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the HSGW service is recognized by the system.Multiple names are needed if multiple HSGW services will be used.
Security Parameter Index Remote Address	**eAN/ePCF IP address:**Specifies the IP address of the eAN/ePCF. The HSGW service allows the creation of a security profile associated with a particular eAN/ePCF.
	SPI number: Specifies the SPI (number) which indicates a security context between the eAN/ePCF and the HSGW.
	Encrypted secret: Configures the shared-secret between the HSGW service and the eAN/ePCF. This command can also be non-encrypted.

Required MAG Context Configuration Information

The following table lists the information that is required to configure the MAG context on an HSGW.

Required Information	Description
MAG context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the MAG context is recognized by the system.
S2a Interface Configuration (To/from P-GW LMA)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system.Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv6 address assigned to the interface.Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17.A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
MAG Service Configuration	
MAG Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the MAG service is recognized by the system.

Required AAA Context Configuration Information

The following table lists the information that is required to configure the AAA context on an HSGW.

Required Information	Description
Gxa Interface Configuration (to PCRF)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system.Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv6 addresses assigned to the interface.Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17.A single physical port can facilitate multiple interfaces.

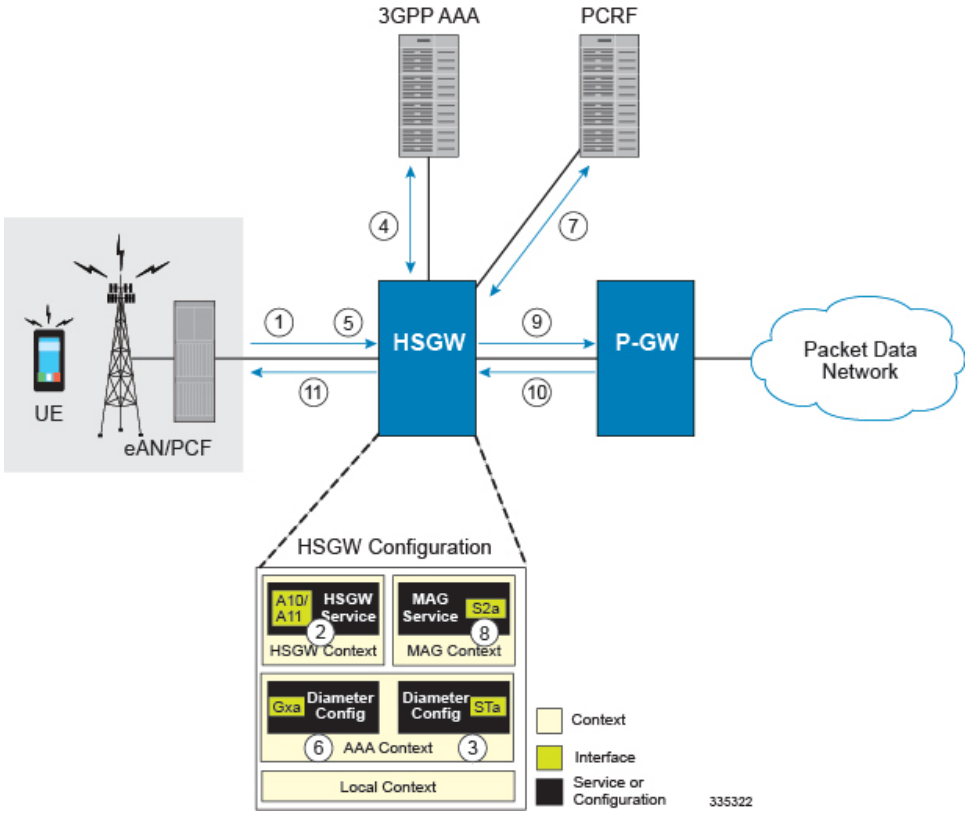
Required Information	Description
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Gxa Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gxa Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters.The realm is the Diameter identity. The originator\'s realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gxa origin host is recognized by the system.
Origin host address	The IPv6 address of the Gxa interface.
Peer name	The Gxa endpoint name described above.
Peer realm name	The Gxa origin realm name described above.
Peer address and port number	The IPv6 address and port number of the PCRF.
Route-entry peer	The Gxa endpoint name described above.
STa Interface Configuration (to 3GPP AAA server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system.Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface.Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17.A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
STa Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the STa Diameter endpoint configuration is recognized by the system.

Required Information	Description
Origin realm name	An identification string between 1 through 127 characters.The realm is the Diameter identity. The originator\'s realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the STa origin host is recognized by the system.
Origin host address	The IPv6 address of the STa interface.
Peer name	The STa endpoint name described above.
Peer realm name	The STa origin realm name described above.
Peer address and port number	The IPv6 address and port number of the PCRF.
Route-entry peer	The STa endpoint name described above.
Rf Interface Configuration (to off-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system.Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface.Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17.A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Rf Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Rf Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters.The realm is the Diameter identity. The originator\'s realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Rf origin host is recognized by the system.
Origin host address	The IPv6 address of the Rf interface.

Required Information	Description
Peer name	The Rf endpoint name described above.
Peer realm name	The Rf origin realm name described above.
Peer address and port number	The IPv6 address and port number of the PCRF.
Route-entry peer	The Rf endpoint name described above.

How This Configuration Works

The following figure and supporting text describe how this configuration with a single source and destination context is used by the system to process a PMIP call originating in the eHRPD network.



Step 1 A subscriber session from the eAN/PCF is received by the HSGW service over the A10/A11 interface.

Step 2 The HSGW service determines which context to use to provide AAA functionality for the session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the System Administration Guide.

Step 3 The AAA group is configured with the Diameter endpoint for the STa interface to the AAA server which is used to authenticate and authorize the subscriber and session.

Step 4 The system completes the Diameter EAP interactions with the AAA server and receives the subscriber profile on successful authentication. The subscriber profile contains Access Point Name (APN) profiles that include APNs the subscriber is authorized to connect to and the P-GW identity/FQDN that serves the APN.

Step 5 Upon successful authentication, the UE begins establishment of PDN connection by sending a Vendor Specific Network Control Protocol (VSNCP) configuration request including the APN and the IP version capability of the UE.

Step 6 The HSGW uses the configured Gxa Diameter endpoint under the IMS Auth service to establish the gateway control session for this PDN.

Step 7 As part of the gateway control session establishment, the HSGW sends a CC-Request (CCR) message to the PCRF and the PCRF acknowledges establishment by responding back with CC-Answer (CCA) message.

Step 8 HSGW uses the configured MAG context to determine the MAG service to use for the outgoing S2a connection.

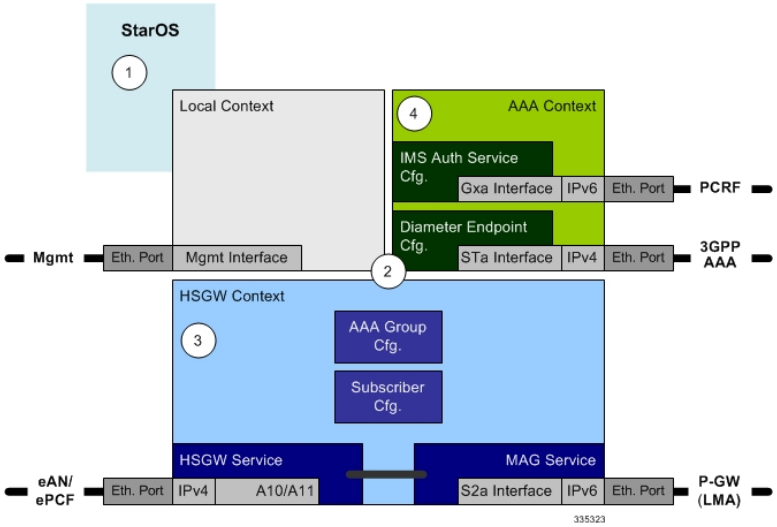
Step 9 The HSGW establishes the S2a connection by sending a PMIP Proxy Binding Update (PBU) to the P-GW including the NAI and APN. The PBU also includes the home network prefix and/or IPv4 home address option based on the subscriber\'s APN profile and UE IP version capability.

Step 10 The P-GW responds with a Proxy Binding Acknowledgement (PBA) that includes the assigned IPv6 home network prefix and interface identifier and/or IPv4 home address acknowledgement option based on the PBU.

Step 11 The HSGW conveys the assigned IP information to the UE in a VSNCP configuration acknowledgement message. Additionally, if an IPv6 address is assign to the UE, the HSGW sends a router advertisement message to the UE including the assigned home network prefix.

Configuration

To configure the system to perform as a standalone HSGW in an eHRPD network environment, review the following graphic and subsequent steps.



Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

Step 2 Set initial configuration parameters such as creating contexts and services by applying the example configurations found in Initial Configuration, on page 9.

Step 3 Configure the system to perform as an HSGW and set basic parameters such as interfaces and an IP route by applying the example configurations presented in HSGW and MAG Service Configuration, on page 11.

Step 4 Create a AAA context and configure parameters for AAA and policy by applying the example configuration in AAA and Policy Configuration, on page 13.

Step 5 Verify and save the configuration by following the instruction in Verifying and Saving the Configuration, on page 15.

Initial Configuration

Step 1 Set local system management parameters by applying the example configuration in Modifying the Local Context, on page 9.

Step 2 Create the context where the HSGW service will reside by applying the example configuration in Creating and Configuring an HSGW Context, on page 10.

Step 3 Specify static IP routes to the eAN/ePCF and/or PDN gateway by applying the example configuration in Configuring Static IP Routes, on page 10.

Step 4 Create an HSGW service within the newly created HSGW context by applying the example configuration in Creating an HSGW Service, on page 11.

Step 5 Create the context where the MAG service will reside by applying the example configuration in Creating and Configuring MAG Context, on page 11.

Step 6 Create a MAG service within the newly created MAG context by applying the example configuration in Creating a MAG Service, on page 11.

Modifying the Local Context

Use the following example to set the default subscriber and configure remote access capability in the local context:

```
configure
     context local
          interface <lcl_cntxt_intrfc_name>
               ip address <ip_address> <ip_mask>
               exit
          server <server-type>
               exit
          subscriber default
               exit
          administrator <name> encrypted password <password> ftp
          ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
          exit
     port ethernet <slot/port>
          no shutdown
          bind interface <lcl_cntxt_intrfc_name> local
          end
```

Notes:

- This configuration is provided as a sample for a configuration file. It is the same configuration that is provided in the "Using the CLI for Initial Configuration" procedure in the Getting Started chapter of the System Administration Guide.
- Remote access is configured using the server command as shown in the local context above. Multiple server types are available. For more information on remote access server types, refer to the Configuring

the System for Remote Access section in the Getting Started chapter of the *System Administration Guide* and the *Context Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Creating and Configuring an HSGW Context

Use the following example to create an HSGW context and Ethernet interfaces, and bind the interfaces to configured Ethernet ports. The interfaces created in this configuration support the A10/A11 connection to the eAN/ePCF and the connection to the P-GW.

```
configure
     context <hsgw_context_name> -noconfirm
          interface <a10-a11_interface_name>
               ip address <ipv4_address>
               exit
          policy accounting <rf_acct_policy_name> -noconfirm
               accounting-level {type}
               operator-string <string>
               exit
          ip domain-lookup
          ip name-servers <ipv4_or_ipv6_address>
          dns-client <name>
          port ethernet <slot_number/port_number>
               no shutdown
               bind interface <a10-a11_interface_name> <hsgw_context_name>
               end
```

Notes:

- The HSGW-to-ePCF (A10/A11) interface must be an IPv4 address.
- Set the accounting policy for the Rf (off-line charging) interface. The accounting level types supported by the HSGW are: PDN, PDN-QCI, QCI, and subscriber. Refer to the *Accounting Profile Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.
- The **ip domain-lookup**, **ip name-servers**, and **dns-client** commands are used during P-GW FQDN discovery.

Configuring Static IP Routes

Use the following example to configure static IP routes for data traffic between the HSGW and the eAN/ePCF and/or P-GW:

```
configure
     context <hsgw_context_name>
          ip route <addr/mask> next-hop <epcf_addr> <hsgw_epcf_intrfc_name>
          ipv6 route <ipv6_addr/prefix> next-hop <pgw_addr> interface
<s2a_intrfc_name>
          end
```

Notes:

- Static IP routing is not required for configurations using dynamic routing protocols.

Creating an HSGW Service

Use the following configuration example to create the HSGW service:

```
configure
     context <hsgw_context_name> -noconfirm
          hsgw-service <hsgw_service_name> -noconfirm
               end
```

Creating and Configuring MAG Context

Use the following example to create a MAG context and Ethernet interface, and bind the interface to configured Ethernet ports. The interface created in this configuration supports the S2a connection to the P-GW.

```
configure
     context <mag_context_name> -noconfirm
          interface <s2a_interface_name>
               ip address <ipv6_address>
               exit
          exit
     port ethernet <slot_number/port_number>
          no shutdown
          bind interface <s2a_interface_name> <mag_context_name>
          end
```

Notes:

- The HSGW-to-PGW (S2a) interface must be an IPv6 address.

Creating a MAG Service

Use the following configuration example to create the MAG service:

```
configure
     context <mag_context_name> -noconfirm
          mag-service <mag_service_name> -noconfirm
               end
```

Notes:

- A separate MAG context with a MAG service can be created to segregate the HSGW network from the MAG network. Refer to Configuring the HSGW Service, on page 12 for additional information on using a MAG service in a separate context.

HSGW and MAG Service Configuration

Step 1 Configure HSGW service settings by applying the example configuration in Configuring the HSGW Service, on page 12.

Step 2 Configure the MAG service by applying the example configuration in Configuring the MAG Service, on page 12.

Configuring the HSGW Service

Use the following configuration example to set parameters including binding the HSGW-eAN/ePCF interface to this service and configuring the SPI between the HSGW and eAN/ePCF:

```
configure
     context <hsgw_context_name> -noconfirm
          hsgw-service <hsgw_service_name> -noconfirm
               mobile-access-gateway context <mag_context_name> mag-service
<mag_service_name>
               associate accounting-policy <rf_name>
               spi remote-address <epcf_address> spi-number <num> encrypted
secret <secret>
               plmn id mcc <number> mnc <number>
               fqdn <domain_name>
               gre sequence-mode recorder
               gre flow-control action resume-session timeout  <msecs>
               gre segmentation
               unauthorized-flows qos-update wait-timeout <seconds>

               bind address <a10-a11_interface_address>
               end
```

Notes:

- The accounting policy is configured in the HSGW context using the **policy accounting** command. This is the pointer to the accounting policy configuration for the Rf (off-line charging) interface. Refer to Creating and Configuring an HSGW Context, on page 10 for more information.
- The **plmn id** command configures Public Land Mobile Network identifiers used to determine if a mobile station is visiting, roaming, or belongs to this network.
- The Fully Qualified Domain Name (FQDN) command is used to identify the HSGW to a P-GW during HSGW selection. The FQDN is included in an APN on the P-GW.
- The **gre** commands are used to configure Generic Routing Encapsulation (GRE) parameters for the A10 protocol.
- The **dns-pgw context** command can be used if the DNS client is configured in a different context from the HSGW service.
- The address used in the binding entry must be the IP address configured as the HSGW-to-ePCF A10/A11 interface in the Creating and Configuring an HSGW Context, on page 10 section.
- The HSGW defaults to a MAG service configured in the same context unless the mobile-access-gateway context <*mag_context_name*> mag-service <*name*> command is used as defined above.

Configuring the MAG Service

Use the following example to configure the MAG service:

```
configure
     context <mag_context_name> -noconfirm
          mag-services <mag_service_name> -noconfirm
               information-element-set custom1
```

```
bind address <s2a_interface_address>
end
```

Notes:

- The information element set is used to identify mobility options sent in PBUs from the MAG to the LMA. "custom1" is custom set of option specific to a Starent customer. The default setting is "standard".
- The address used in the binding entry must be the IP address configured as the HSGW-to-PGW S2a interface in the Creating and Configuring an HSGW Context, on page 10 section.

AAA and Policy Configuration

Step 1 Configure AAA and policy interfaces by applying the example configuration in Creating and Configuring the AAA Context, on page 13.

Step 2 Configure the default subscriber for the AAA context by applying the example configuration in Modifying the Default Subscriber, on page 14.

Step 3 Create and configure QCI to QoS mapping by applying the example configuration in Configuring QCI-QoS Mapping, on page 14.

Creating and Configuring the AAA Context

Use the following example to create and configure a AAA context including diameter support and policy control, and bind ports to interfaces supporting traffic between this context and a AAA server and PCRF:

```
configure
     context <aaa_context_name> -noconfirm
          interface <aaa_sta_ipv4_interface_name>
               ip address <ipv4_address>
               exit
          interface <pcrf_gxa_ipv6_interface_name>
               ip address <ipv6_address>
               exit
          interface <ocs_rf_ipv4_interface_name>
               ip address <ipv4_address>
               exit
          subscriber default
               exit
          aaa group default
               diameter accounting endpoint <rf_ofcs_server>
               diameter authentication endpoint <sta_cfg_name>
               diameter accounting server <rf_ofcs_server> priority <num>
               diameter authentication server <3gpp_aaa_server> priority <num>
               exit
          ims-auth-service <gxa_ims_service_name>
               policy-control
                    diameter origin endpoint <gxa_cfg_name>
                    diameter dictionary <gxa_dictionry_name>
                    diameter host-select table <> algorithm round-robin
                    diameter host-select row-precedence <> table <> host
```

```
<gxa_cfg_name>
                    exit
               exit
          aaa group default
               diameter authentication dictionary <name>
               diameter authentication endpoint <sta_cfg_name>
               diameter authentication server <sta_cfg_name> priority <>
               exit
          diameter endpoint <sta_cfg_name>
               origin realm <realm_name>
               origin host <name> address <aaa_ctx_ipv4_address>
               peer <sta_cfg_name> realm <name> address <aaa_ipv4_address>
               route-entry peer <sta_cfg_name>
               exit
          diameter endpoint <gxa_cfg_name>
               origin realm <realm_name>
               origin host <name> address <aaa_ctx_ipv6_address>
               peer <gxa_cfg_name> realm <name> address <pcrf_ip_addr> port <>
               route-entry peer <gxa_cfg_name>
               end
          diameter endpoint <rf_cfg_name>
               origin realm <realm_name>
               origin host <name> address <aaa_ctx_ipv4_address>
               peer <rf_cfg_name> realm <name> address <ocs_ip_addr> port <>
               route-entry peer <rf_cfg_name>
               end
```

Modifying the Default Subscriber

Use the following example to modify the default subscriber configuration in the AAA context:

```
configure
     context <aaa_context_name> -noconfirm
          subscriber default
               ims-auth-service <gxa_ims_service_name>
```

Notes:

- The IMS Auth Service is also crested and configured in the AAA context.

Configuring QCI-QoS Mapping

Use the following example to create and map QCI values to enforceable QoS parameters:

```
configure
     qci-qos-mapping <name>
          qci 1 user-datagram dscp-marking <hex>
          qci 3 user-datagram dscp-marking <hex>
          qci 9 user-datagram dscp-marking <hex>
          exit
```

Notes:

- QCI values 1 through 9 are standard values and are defined in 3GPP TS 23.203. Values 10 through 32 can be configured for non-standard use.

- The configuration example shown above only shows one keyword example. Refer to the *QCI - QOS Mapping Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on the **qci** command and other supported keywords.

Verifying and Saving the Configuration

Save your HSGW configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring Optional Features on the HSGW

The configuration examples in this section are optional and provided to cover the most common uses of the HSGW in a live network. The intent of these examples is to provide a base configuration for testing.

Configuring Network Initiated QoS

The configuration example in this section enables the ability to use network initiated QoS functionality.

In HSGW Service Configuration Mode, configure network initiated QoS as follows:

```
configure
     context <hsgw_context_name> -noconfirm
          hsgw-service <hsgw_service_name> -noconfirm
               network-initiated-qos
               rsvp max-retransmissions <count>
               rsvp retransmission-timeout <seconds>
               end
```

Notes:

- The **rsvp max-retransmissions** command specifies the maximum retransmission count of RP control packets. <*count*> must be an integer value between 1 and 1000000. Default count is 5.
- The **rsvp retransmission-timeout** command specifies the maximum amount of time, in seconds, to allow for retransmission of RP control packets. <*seconds*> must be an integer value between 1 and 1000000. Default is 3 seconds.